International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 7 4972 - 4976

Bio-Cryptosystem Using Fuzzy Vault Scheme

Arzoo Arora
Department of Information Technology
K.J Somaiya College of Engineering
Mumbai, Maharashtra
arzooarora.arora7@gmail.com

Prof. Ravindra Divekar
Department of Information Technology
K.J Somaiya College of Engineering
Mumbai, Maharashtra
ravindradivekar@somaiya.edu

***Abstract*—** In recent years most challenging problem is protection of information from unauthorized users. The conventional Cryptographic systems are insufficient to provide a security. The main problem is how to protect private keys from attackers and Intruder such as in case of Internet Banking. Cryptographic systems have been widely used in many information security systems. Hence in this paper we have proposed a framework of Biometric based cryptosystems. It provide reliable way of hiding private keys by using biometric features of individuals. A fuzzy vault approach is used to protect private keys and to release them only when legitimate individual enter their biometric sample. The main advantage of this system is there is no need of storing biometric information. However, fuzzy vault systems do not store directly these templates since they are encrypted with private keys by using novel cryptography algorithm. In proposed framework we are combining iris features with the encryption algorithm that can be a new research direction. The proposed approach provides high security and also image information can be protected.

Keywords- *Cryptographic template, biometric, feature extraction, wavelet transform*

*****

I. INTRODUCTION

Nowadays the most challenging problem is to protect information from unauthorized users. The conventional Cryptographic systems are insufficient to provide a suitable security. The main problem is protection of user private keys from attackers. Many researcher try to solve this problem using cryptographic approach. Recently, Bio-cryptosystems have been introduced as a reliable way of hiding private keys by using biometric templates of person. The different biometric traits can be used such as iris, fingerprint, face, ear etc. The enhancement of security is performed using fuzzy vault that refers to a biometric cryptosystem used to protect private keys of user at the time of authentication. However, fuzzy vault systems do not store directly these templates since they are encrypted with private keys by using encryption algorithm. Previous fuzzy vault systems were designed by using fingerprint, face, and so on. However, there has very less fuzzy vault system that can be made using iris. It is a well-known fact that iris is the most reliable biometric compare to other biometric traits and also discriminate between persons. This paper is organized into the following sections. Section 1 gives an introductory part and importance of information security system. Section 2 describes various types of existing system design to protect the information. Section 3 presents a detailed discussion on proposed system. Finally, Section 4 concludes this paper.

II. LITERATURE SURVEY

Conventional methods for personal identification are based on token based password, physical key, ID card, secret password, etc. These methods have disadvantages such as keys may be lost, passwords may be forgotten. Hence researcher primary focus is on biometric features personal identification system [1]. Youn Joo Lee et al.[2] proposed the Fuzzy vault scheme to protect information. Raghu and Deepthi [3] has provide solution Security requirements demand that these systems be operated with very large secret keys. Since it is very difficult to remember large private keys, these keys are stored by using biometric features and this is called biometric encryption. They propose a multimodal biometrics based encryption scheme. Here combine features of fingerprint and iris with a user defined secret key. It is experimentally verified that the proposed system outperforms unimodal biometric encryption systems. Sanjay Kanade et al. [4] has proposed smart card, iris code and password based scheme for cryptographic key regeneration. In this approach error correcting codes i.e. Hadamard is used that can correct up to 25% error and regenerate the 198-bit key with estimated entropy of 83 bits on the NIST-ICE iris database at 0.055% False Acceptance Rate (FAR) and 1.04% False Rejection Rate (FRR). Xiukun Li[5] proposed the novel biometric features based encryption approach, which can improve the traditional cryptography flows. In this approach 256 bit textural feature vector is extracted from the normalized image by using a 2-D Gabor filters. And then the arithmetic operations and Reed-Solomon error-correcting algorithm are employed to directly encrypt and decrypt the data. Experimental results demonstrate the feasibility of the proposed system. Sim Hiew Moi[6] present an approach to generate a more secure and unique key from iris template. The AES cryptography algorithm are employed for encrypt and decrypt the identity data. Distance metric such as hamming distance and Euclidean distance are used for the template matching identification process. Experimental results show that this system can obtain a higher security with a low false rejection or false acceptance rate. Sanjay Kanade[7] proposed the combined approach of iris and face to obtain a long cryptographic key of 210 bit having high 183 bit entropy value significantly higher than the 83-bit entropy obtained for

iris), at a False Acceptance Rate of 0% and a False Rejection Rate of 0.91%. Radha Narayanan[8] proposed Fuzzy vault system based on fingerprint and security is enhanced using double encryption technique by means of combining symmetric key and a symmetric key generation. Also, Reed and Solomon codes are used to provide tolerance for decryption. Wei Wei et al.[9] solves the problem of memory and storage problem of long key in encryption algorithm, so combined biometric characteristic with the traditional encryption algorithm is a new research direction. An encryption algorithm based on key from iris features and by 2D Haar wavelet features are extracted. 375-bit iris codes is generated, 128-bit key is extracted from iris codes by using unit mapping function. The encryption and decryption experiments with AES was applied on the image with size of 512×512. Experimental result shows that the encrypted image has high security, also the image information is protected. A.Jagadeesan [10] proposed a novel cryptographic approach of key generation using multiple biometric traits I.e. iris and fingerprint. Initially, minutiae points and texture properties are extracted from the fingerprint and iris images respectively. Subsequently, the extracted features are fused together at the feature level to construct the multi-biometric template. Finally, a 256-bit secure cryptographic key is generated from the multi-biometric template. The experimental results demonstrate the effectiveness of the proposed approach on CASIA database.

III. PROPOSED METHODOLOGY

The proposed framework is divided into different steps: Iris pre-processing, feature Extraction and Iris recognition.

A. Iris Preprocessing

Iris recognition is the most precise and fastest of the biometric authentication method, the iris recognition

1) Image Acquisition:

First step is image acquisition, the image is taken for further processing, in our project we have used standard CASIA database for iris.

2) Localization:

The acquired iris image has to be preprocessed to detect the iris, which is an annular portion between the pupil (inner boundary) and the sclera (outer boundary).The task consists of localizing the inner and outer boundaries of the iris, both are circular, but the problem lies in the fact that they are not co-centric .It is necessary to calculate the two circles parameters separately. The first step in iris localization is to detect pupil which is the black circular part surrounded by iris tissues. The center of pupil can be used to detect the outer radius of iris patterns. The important steps involved are: [i] Pupil detection(inner boundary) and [ii] Outer iris localization(outer boundary)

a) Pupil Detection: The iris image is converted into grayscale to remove the effect of illumination. As pupil is the largest black area in the intensity image, its edges can be detected easily from the binaries image by using suitable threshold on the intensity image. But the problem of binarization arises in case of persons having dark iris. Thus the localization of pupil fails in such cases.

i. Hough Transformation: In order to overcome these problems Circular Hough Transformation for pupil detection can be used. The basic idea of this technique is to find curves that can be parameterized like straight lines, polynomials, circles, etc., in a suitable parameter space. The Hough transform is an image processing technique which is effective in determining the parameters of simple geometric shapes. The circular Hough transformation is applied to compute the radius and center.

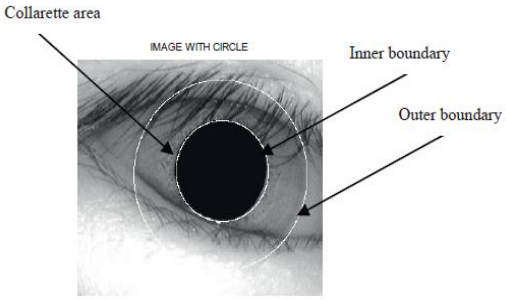

Figure 1. Diagram shows the detection of circles (inner and outer boundary) for an image

Coordinates of the circular iris and pupil regions. The transformation is able to overcome artifacts such as shadows and noise. The approach is found to be good particularly dealing with all sorts of difficulties including severe occlusion. Hough transformation is applied for computing the parameters of circles passing through each edge point. The parameters such as the center coordinates (xc, yc) and the radius r, define a circle according to the following equation.

$$(x- xc)2 + (y - yc)2 = r\ 2$$

ii. Outer Iris Localization: External noise is removed by blurring the intensity image. But too much blurring may dilate the boundaries of the edge or may make it difficult to detect the outer iris boundary, separating the eyeball and sclera. This contrast enhanced image is used for finding the outer iris boundary by drawing concentric circles, as shown in Figure of different radii from the pupil center and the intensities lying over the perimeter of the circle are summed up. Among the candidate iris circles, the circle having a maximum change in intensity with respect to the previous drawn circle is the iris outer boundary.

3) Segmentation:

Segmentation follows localization to separate eyelid and eyelashes portion from actual iris part. Our iris segmentation technique is based on the well known circular Hough transform method but we make a number of improvements and optimizations that serve both to improve the accuracy of the results and speed up execution. As before,

 ISSN: 2321-8169
4972 - 4976

we use downscaled images to reduce the compute time required The success of segmentation depends on the imaging quality of eye images. The persons with darkly pigmented irises will present very low contrast between the pupil and iris region if imaged under natural light, making segmentation more difficult. The segmentation stage is critical to the success of an iris recognition system, since data that is falsely represented as iris pattern data will corrupt the biometric templates generated ,resulting in poor recognition rates.

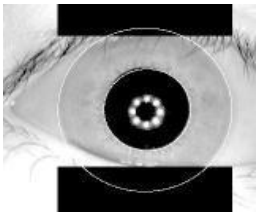

Figure 2. Iris Segmentation

iii. *Canny Edge Detection:* Canny edge detection starts with linear filtering to compute the gradient of the image intensity distribution function and ends with thinning and Thresholding to obtain a binary map of edges. One significant feature of the canny operator is its optimality in handling noisy images as the method bridges the gap between strong and weak edges of the images by connecting the weak edge in the output only if they are connecting to strong edges. In iris segmentation, an edge map is created by computing the first Derivatives of intensity values in an iris image and then performing Thresholding on the result. Then these iris segmentation algorithms achieve high performance on iris database images captured in favorable conditions. The images are collected under constrained environment with good lighting and with subject's cooperation (eyes wide open). In these high quality iris images, various noise factors are minimized by using suitable image acquisition techniques.

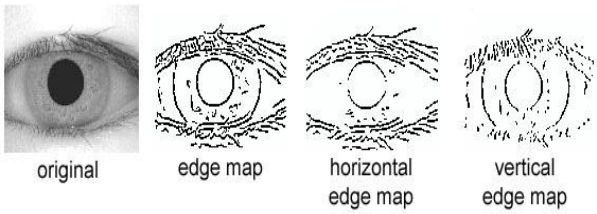

Figure 3. a) an eye image (020_2_1 from the CASIA database) b) corresponding edge map c) edge map with only horizontal gradients d) edge map with only vertical gradients.

4) Normalization:

As the Iris is a circular part which maybe of different dimension for every image. Image is captured in different size, for the same person also size may vary because of the variation in illumination and other factors. The normalization process will produce iris regions, which have the same constant dimensions, so that two photographs of the same iris under different conditions will have Characteristic features at the same spatial location. For normalization we used the Daugman rubber sheet modal in this we convert the circular image into rectangular form with the size 20 x 240 i.e. vertically 20 and horizontally 240 pixel.

Figure 4. Normalized Iris Image

iv. *Daugman's rubber sheet modal:* The concept of rubber sheet modal suggested by Daugman's takes into consideration the possibility of pupil dilation and appearing of different size in different images. For this purpose, the coordinate system is changed by unwrapping the iris and mapping all the points within the boundary of the iris into their polar equivalent as shown in Figure 5. The mapped image has 20 × 240 pixels. It means that the step size is same at every angle.

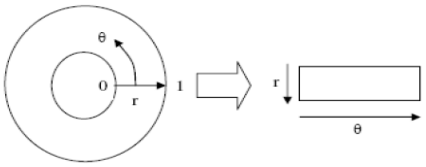

Figure 5. The Polar System

$$I(x(\rho,\theta), y(\rho,\theta)) \rightarrow I(\rho,\theta)$$

with

$$x_p(\rho,\theta) = x_{\rho 0}(\theta) + r_p * \cos(\theta)$$
$$y_p(\rho,\theta) = y_{\rho 0}(\theta) + r_p * \sin(\theta)$$
$$x_i(\rho,\theta) = x_{i0}(\theta) + r_i * \cos(\theta)$$
$$y_i(\rho,\theta) = x_{i0}(\theta) + r_i * \sin(\theta)$$

where rp and ri are respectively the radius of pupil and the iris, while (xp(θ), yp(θ)) and (xi(θ), yi(θ)) are the coordinates of the pupillary and limbic boundaries in the direction θ. The value of θ belongs to [0;2π], ρ belongs to [0;1]. Libor Masek thesis [11]

B. Feature Extraction:

The Fourier transform has been the most commonly used tool for analyzing frequency properties of a given signal, while after transformation, the information about time is lost and it's hard to tell where a certain frequency occurs. To solve this problem, we can use kinds of time-frequency analysis techniques learned from the course to represent a 1-D signal in time and frequency simultaneously. There is always

 ISSN: 2321-8169
4972 - 4976

uncertainty between the time and the frequency resolution of the window function used in this analysis since it is well know that when the time duration get larger, the bandwidth becomes smaller. Several ways have been proposed to find the uncertainty bound, and the most common one is the multiple of the standard deviations on time and frequency domain.

C. *Iris Recognition*

In the presented work, we are combining biometric features with the encryption algorithm that can be a new research direction. The proposed approach provides high security and avoid unauthorized access. The proposed system is divided into two parts i.e. [i] Enrollment phase and [ii] Verification phase depicted as follows:

1) *Enrollment Phase*

Figure 5 describes the enrollment phase, the first step is the iris image acquisition. Before feature extraction, iris pre-processing [10] is performed to get desired transformed image for feature extraction. The preprocessing step includes 1) iris localization, segmentation, performed using Hough Transformed and 2) Normalization of the image are performed using the Daugmans' rubber sheet model. After pre-processing circular iris get converted to rectangular box linear image. Then features are extracted such as texture, color, features using Gabor wavelet transformation. And then Fuzzy vault encoding is performed, in this, the user input private key is combined with iris features using novel cryptographic algorithms and cryptographic template is generated. In this step element of extracted biometric features get retrieve according to the position and bit value of private key values and these extracted bits get merged with features and private key of individuals. These templates are secure and avoid biometric template storage problems.

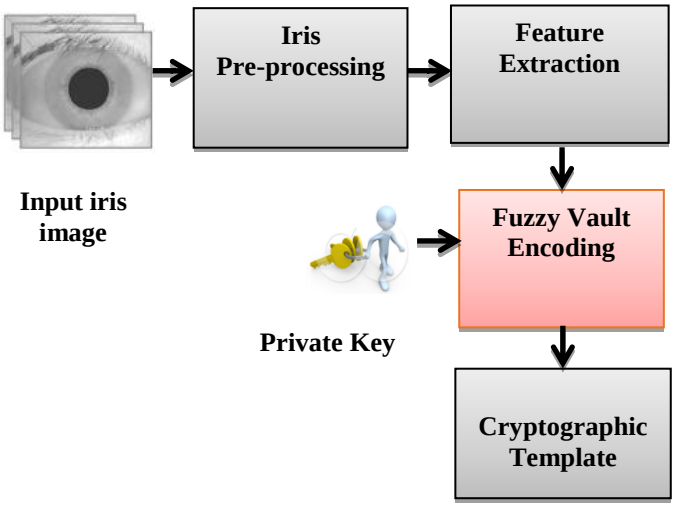

Figure 5. Enrollment Phase

2) *Verification Phase*

Figure 6 describes the verification phase, the first step is the iris image acquisition. Before feature extraction, iris pre-processing is performed to get desired transformed image for feature extraction. Then Fuzzy vault decoding is performed, in this, cryptographic template is generated and also that template is matched with the database templates. After template matching legitimate person id and private key are extracted. For a matching Hamming distance matcher or KNN can be used. In the matching phase three level security is provided 1) Private key matching, 2) If matched private key of legitimate individual, then biometric features are matched, 3) If template information is matched in two levels, then in third level, cryptographic template is matched else the user is categories as an imposter.

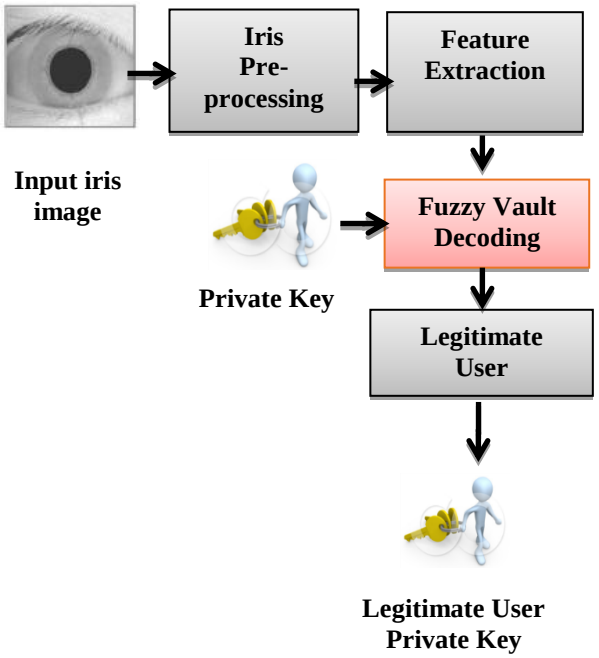

Figure 6: Verification phase

IV. CONCLUSION

In this paper we have proposed biometric based security system using Fuzzy fault encoding and decoding approach the cryptographic templates are generated that enhances the security of system. The main aim is to identify legitimate individuals from group of people and developed secure authentication system. We are challenging existing work but it's an attempt to protect system from attackers and intruders.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video Based Biometrics, vol. 14, no. 1, pp. 4–20, 30 January 2004.

[2] Youn Joo Lee, Kang Ryoung Park, Sung Joo Lee, "A new method for generating an Invariant iris Private key based on the fuzzy vault system", IEEE transaction on Systems, Man, and Cybernetics, vol. 38, no. 5, October 2008.

[3] I. Raglu and Deepthi P.P, "Multimodal Biometric Encryption Using Minutiae and Iris feature map", Proceeding of IEEE Conference on Electrical, Electronics and Computer Science, Madhya Pradesh, pp. 926-934, 2012.

[4] Sanjay Kanade, Danielle Camara et al., "Three factor scheme for biometric-based cryptographic key Regeneration using iris", Biometrics Symposium, pp. 59-64, 23-25 Sept. 2008

[5] Xiukun Li, Xiangqian Wu, "A Novel Cryptographic Algorithm based on Iris Feature", IEEE International conference on

Computational intelligence and Security, pp. 463-466, 13-17 Dec. 2008

[6] Sim Hiew Moi, "Iris Biometric Cryptography for Identity Document", International Conference of soft computing and Pattern Recognition, pp. 736-741, 4-7 Dec. 2009.

[7] Sanjay Kanade, Dijana Petrovska-Delacretaz," Obtaining Cryptographic Keys Using Feature Level Fusion of Iris and Face Biometrics for Secure User Authentication", Computer vision pattern recognition workshop, pp. 138-145, 13-18 June 2010.

[8] Radha Narayanan, S.Karthikeyan,"Obtaining Cryptographic Keys Using Feature Level Fusion of Iris and Face Biometrics for Secure User Authentication", Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering , March 21-23, 2012

[9] Wei Wei, Zhou Jun," Image encryption algorithm Based on the key extracted from iris Characteristics", 14th IEEE International Symposium on Computational Intelligence and Informatics • 19–21 November, 2013, Budapest, Hungary

[10] A. Jagadeesan, K. Duraiswamy, "Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris", International Journal of Computer Science and Information Security, Vol. 7, No. 2, February 2010

[11] L. Masek, "Recognition of Human Iris Patterns for Biometrics Identification", B.E. thesis, School of Computer Science and Software Engineering, University of Western Australia, 2003.